Völkerrechtsblog
Der Blog des Arbeitskreises junger Völkerrechtswissenschaftler*innen

DIGITAL SURVEILLANCE AND CYBER ESPIONAGE SYMPOSIUM

Unilateralism ahead?

Human rights, digital surveillance and the "extraterritorial question" in international law

MILAN TAHRAOUI — 12 December, 2016

Here we are. It could seem a bit obvious to start with this overwhelming event, but it is truly important to stress that the recent results of the US elections will have far reaching consequences in many fields of international law, including the one that this post is dealing with: the yet unsettled complex set of issues of extraterritoriality with respect to surveillance practices. Indeed, one of the foreseeable developments to be expected at the international level is a reaffirmation (even an increase) of a clear unilateralist agenda for digital surveillance activities practised by the US security and intelligence agencies in the near future. This is not new: the United States are among the few States that have explicitly rejected any extraterritorial human rights

obligations, despite the large consensus existing in international law. It would nevertheless be wrong to assume that the US is the only country that exhibits such unilateralist attitudes (broadly speaking) as to the regulation (or its absence) of extraterritorial digital activities. On the contrary, what should already be stressed is that this type of unilateralist attitudes is well-established, including on the side of the EU (for the purpose of this post, the EU is treated like a State in its capacity to act unilaterally). This contribution argues that from the viewpoint of human rights protection, unilateralism can translate both in an increasing chance to ensure a more effective protection, but also in the risk to interfere with much needed truly international standards for dealing with digital surveillance. For some, the current situation looks even more like the "law of the jungle" than in other fields of international law.

The internet as a battlefield of competing claims and normative ideas

Why do European States resort to unilateral measures to extend the human rights protection against surveillance practices beyond their boarders? The background is the very unsettled nature of the current state of affairs under international law, resulting in a lack of protection. It is not argued here that there is a legal vacuum but rather that the rules at the international level dealing with the complex questions at stake, especially when extraterritoriality is involved, have not yet stabilised (see here for a similar discussion on international norms and cybersecurity). In practice as much as in the literature, a lot of questions remain unsettled. The set of issues implied by the extraterritorial question has been, for example, touched upon by the European Court of Human Rights without the Court

however had directly confronting itself with the question of whether there exist extraterritorial human rights obligations for the international digital surveillance activities of States. There are however pending cases before the Strasbourg Court that are offering an opportunity to cope with this issue.

This implies that we are in a momentum where the legal determination as to the type of authority that might be exercised by States outside the confines of their territories and through digital activities requires one to delve into normative pluralism. This implies an effort of construing issues according to various norms or standards that are proposed or developed in multiple fora. Also, it concretely means the existence of influence struggles between different models emanating from various types of States, NGOs, specialised bodies or private corporations or experts. Transatlantic relations show that serious disagreements exist as to which human rights or general interest objectives should be prioritised, while both the US and the EU are openly embracing common views on some objectives (such as multistakeholderism). Although some scholars have relied on a reasonableness-based type of rules for the exercise of State jurisdiction in the Internet era, it is still unclear whether the US will favour such a path for the ongoing reform of its rules of conflicts of jurisdictions and laws. Considering this, conflict of models or spheres of influence will exert an ever-increasing important role in the shaping of future international norms applicable to those questions (in this sense, see here at "1.").

The "extraterritorial question" under international law in the digital age: could unilateralism be a solution?

Since international law does not contain clear rules to face the serious challenges relating to extraterritorial surveillance or protection against it, could unilateralism play a positive role on the discrepancy existing between the plurality of normative claims?

Unilateralism is understood here as a type of actions and approaches undertaken or developed by States which aims at fulfilling some of their national interests without or against existing multilateral or international legal frameworks in an individualistic fashion (akin to theories of political realism in international relations). Unilateralism can rely on diverse strategies, among which extraterritoriality plays a key role in a twofold manner: first, when States assert extraterritorial (or territorially expanded) jurisdictional claims over transnational digital activities that have a connection with their territory or by relying on other criteria including the nationality principle and some variations of the effects doctrine; secondly, by denying the existence or construing in a very narrow manner the applicability of human rights obligations for extraterritorial digital activities, which is especially the case for surveillance at large (see here and here).

Unilateralism is not per se to be rejected in the context of human rights protection against surveillance. As the example of the EU action in this field shows, it can be claimed that despite the emergence of international human rights standards applicable to digital surveillance activities, a big part of the effective human rights protection in fact relies on domestic legislation (due to the core principle of subsidiarity in international human rights law). Optimistically, it could be said that unilateralism is part of the international human rights protection “toolbox” that should include international

law, but also European and domestic laws. It has been argued here that the intensification of EU data protection and privacy fundamental rights as well as their territorial extension could translate into an increasing level of human rights obligations for EU extraterritorial digital actions. This is one of the reasons why the UN Special Rapporteur on the Right to Privacy has called for a mix of unilateralism and regional as well as global cooperation for the manifold protection of the private sphere in our digitalised societies.

Despite its pitfalls, unilateralism could prevail over cooperative attempts

However, there are certain risks associated with this type of action and it is argued here that unilateralism might be detrimental to a more multilateral/global agenda (see an initiative in this sense here).

Firstly, one line of argumentation pushed forward by scholars, experts of the Internet governance, or NGOs is that unilateral actions can reinforce what is called "national digital sovereignty" or the "balkanization of the internet" and go in the direction of a "re-territorialisation" of the internet. Critics of such a tendency say that this endangers the openness, interconnectivity and global nature of the Internet. The ECJ Google Spain case saga offers an interesting case in this constellation (see for example here).

In the transatlantic context, if one assumes that the unilateralist attitude of the US will increase, counter-reactions are to be expected. In the context of economic interests, there already exists a French Parliamentarian Commission dealing with the extraterritorial imposition of US laws. Furthermore, it is questionable whether consensus on these questions is achievable. France and Germany have

several times attempted to implement a "digital sovereign" approach. These two States can generally be said to pursue converging interests at the international level, but as the negotiations of the Data Protection General Regulation and the Privacy Shield show (see the contribution of Clément Perarnaud), serious divergences are still observable.

Germany is one example of a State pushing for an agenda where both global and unilateral (national and European) objectives are pursued for digital activities in international law. Indeed, under the name of Völkerrechts des Netzes (international law of networks) Germany is strongly backing the development of multilateral rules for the regulation of digital activities while asserting at the same time that there is a need to recover "digital sovereignty" and to facilitate the expansion of European rules internationally (here, esp. at 103—104). However, France has recently undertaken several reforms that are mainly serving security interests over privacy ones (see here, here and here), even though independent administrative authorities such as the CNIL exert a positive influence on privacy interests.

This raises doubts whether even inside the European common legal space, common regional interests can survive agendas of single national States. If unilateralism continues to spread, what should be expected in terms of convergence and global standards for the regulation of digital surveillance activities? It seems indeed possible that the former forgoes the latter, given the ambivalences among States that are apparently sharing more general objectives, such as the European States.

More generally, claims made for unilateral approaches in this context can have the effect of reinforcing long-standing

claims for a sovereign-based international approach to the digital environment. Ambiguity that exists on the side of "democratic-liberal" States about the way to proceed could make a case for other States trying to anchor sovereign rights on "their portion of the Internet". Already, the priority given to national security, cybersecurity and international security interests feeds a trend where the existing deep gap seems to be decreasing. Thus, a consensus could emerge on some controversial points due to the wide-spread phenomenon of securization, without "compensatory" constraints against extraterritorial surveillance abuses. Proposals have indeed been made by global cyber powers to foster and embed national security (among others) interests into new rules for the digital environment (see for example here). This is even more the case with the concept of informational security pushed forward by the Shanghai Cooperation Organisation before the UN (it can be read in light of this prognosis). Opposition remains strong, including from European States. However, some calls for a better coordination of US and Chinese unilateral interests over "cyberspace" (for example, here) might result in a higher degree of influence on those issues than multilateral standards for the regulation of surveillance or than a truly global agenda.

Given its dark sides, unilateralism should be treated with caution. That said, recent developments and the overall trend to "securization" do not point in the direction of a global multilateral solution (for a better protection of individuals against surveillance practices) in the near future, incentivising in turn unilateralism, among others, in Europe for achieving this very goal…

Milan Tahraoui is a doctoral candidate in international law both at Paris 1 Pantheon-Sorbonne University and Freie Universität zu Berlin as well as a research fellow of the Max Planck Institute for Comparative Public Law and International in Heidelberg.

This contribution corresponds to a presentation which has first been given at a colloquium on digital surveillance and cyber espionage, which took place from 22nd to 23rd September in Paris. Additional contributions can – in addition to those on the Völkerrechtsblog (here) – be found here and here.

ISSN 2510-2567

Tags: *Cyber*, *Digitalization*, *Human Rights*

Related

The surveillance you have paid for
5 December, 2016
In "Digital surveillance and cyber espionage"

Gunneflo Book Symposium: Part 3
22 March, 2017
In "Gunneflo Book Symposium"

Beyond Human Rights – Beyond International Law?
20 January, 2016
In "Debating "Beyond Human Rights""

PREVIOUS POST
Der Schutz der Menschenrechte im Cyberspace durch die EMRK

NEXT POST

Open Access on the shores of international legal scholarship

No Comment

Leave a reply

Logged in as ajv2016. Log out?

SUBMIT COMMENT

☐ Notify me of follow-up comments by email.

☐ Notify me of new posts by email.